What is claimed is:

1. A method of multipoint delivery of encoded digital data from an upstream system to specific destinations in a downstream system, comprising the steps of:

encrypting digital data by the use in said upstream system of an encryption key;

generating, on the basis of said encryption key, a plurality of pieces of key information, respective pieces of said key information being specific to each of said specific destinations;

delivering said respective pieces of key information to each of said specific destinations over a plurality of delivery routes that differ from routes used to deliver said digital data and that differ from each other;

delivering said encrypted, encoded digital data;

receiving said encrypted, encoded digital data and said pieces of key information by a decryption server at said downstream system, said decryption server being accessed only by authorization;

restoring said encryption key based on the received pieces of key information;

using the restored encryption key to decrypt the received digital data;

locally generating a scramble key and a descramble key if the received digital data is successfully decrypted;

decoding the decrypted digital data to output restored digital data;

using the locally generated scramble key to scramble said restored digital data;

descrambling the scrambled digital data by an output device at said downstream system using the descramble key generated by said decryption server, said output device being accessed only by authorization; and

outputting from said output device the descrambled digital data in a predetermined output format.

2. . A method of multipoint delivery of encoded digital data from an upstream system to specific destinations in a downstream system, comprising the steps of:

encrypting digital data by the use in said upstream system of an encryption key;

generating, on the basis of said encryption key, sets of passkeys specific to said specific destinations;

delivering either a set of passkeys or passkey information, from which said passkeys may be reproduced, to a respective destination over a plurality of delivery routes that differ from routes used to deliver said digital data and that differ from each other;

delivering said encrypted, encoded digital data;

receiving said encrypted, encoded digital data and said set of passkeys or passkey information by a decryption server at said downstream system, said decryption server being accessed only by authorization;

restoring said encryption key based on the received pieces of key information;

using the restored encryption key to decrypt the received digital data;

locally generating a scramble key and a descramble key if the received digital data is successfully decrypted;

decoding the decrypted digital data to output restored digital data;

using the locally generated scramble key to scramble said restored digital data;

descrambling the scrambled digital data by an output device at said downstream system using the descramble key generated by said decryption server, said output device being accessed only by authorization; and

outputting from said output device the descrambled digital data in a predetermined output format.

3. A method of multipoint delivery of encoded digital data from an upstream system to specific destinations in a downstream system, comprising the steps of:

encrypting digital data by the use in said upstream system of an encryption key;

generating on the basis of said encryption key, a set of passkeys specific to each of said specific destinations;

generating a plurality of partial keys based on a portion of the passkeys in said set or a portion of passkey information from which said passkeys may be reproduced;

delivering either said plurality of partial keys or partial key information from which said partial keys may be reproduced, and delivering the remaining passkeys not used to generate said partial keys or the remaining passkey information, to each of said specific destinations over a plurality of delivery routes that differ from routes used to deliver said digital data and that differ from each other;

delivering said encrypted, encoded digital data;

receiving said encrypted, encoded digital data, said partial keys or partial key information and said remaining passkeys or passkey information by a decryption server at said downstream system, said decryption server being accessed only by authorization;

restoring said encryption key using either the received partial keys or partial key information and using either said remaining passkeys or said remaining passkey information delivered over said plurality of delivery routes;

using the restored encryption key to decrypt the received digital data;

locally generating a scramble key and a descramble key if the received digital data is successfully decrypted;

decoding the decrypted digital data to output restored digital data;

using the locally generated scramble key to scramble said restored digital data;

descrambling the scrambled digital data by an output device at said downstream system using the descramble key generated by said decryption server, said output device being accessed only by authorization; and

outputting from said output device the descrambled digital data in a predetermined output format.

4. A method of multipoint delivery of encoded digital data from an upstream system to specific destinations in a downstream system, comprising the steps of:

encrypting digital data by the use in said upstream system of a first encryption key;

generating second encryption keys specific to respective destinations and/or to the content of said digital data;

using said second encryption key to encrypt either said first encryption key or first encryption key information from which said first encryption key may be reproduced;

delivering either said encrypted first encryption key or said encrypted first encryption key information and delivering either said second encryption key or second encryption key information from which said second encryption key may be reproduced, to respective destinations over a plurality of delivery routes that differ from routes used to deliver said digital data and that differ from each other;

delivering said encrypted, encoded digital data;

receiving said encrypted, encoded digital data, said encrypted first encryption key or first encryption key information and said second encryption key or second encryption key information by a decryption server at said downstream system, said decryption server being accessed only by authorization;

restoring said first encryption key by decrypting the received encrypted first encryption key or first encryption key information by use of the received second encryption key or second encryption key information;

using the restored encryption key to decrypt the received digital data;

locally generating a scramble key and a descramble key if the received digital data is successfully decrypted;

decoding the decrypted digital data to output restored digital data;

using the locally generated scramble key to scramble said restored digital data;

descrambling the scrambled digital data by an output device in said downstream system using the descramble key generated by said decryption server, said output device being accessed only by authorization; and

outputting from said output device the descrambled digital data in a predetermined output format.

5. A method of multipoint delivery of encoded digital data from an upstream system to specific destinations in a downstream system, comprising the steps of:

encrypting digital data by the use in said upstream system of a first encryption key;

generating second encryption keys specific to respective destinations and/or to the content of said digital data;

using said second encryption key to encrypt either said first encryption key or first encryption key information from which said first encryption key may be reproduced;

generating, on the basis of said second encryption key, a set of passkeys;

delivering either said encrypted first encryption key or said encrypted first encryption key information and delivering either said set of passkeys or passkey information, from which said set of passkeys may be reproduced, to each of said specific destinations over a plurality of delivery routes that differ from routes used to deliver said digital data and that differ from each other;

delivering said encrypted, encoded digital data;

receiving said encrypted, encoded digital data, said encrypted first encryption key or first encryption key information and said set of passkeys or passkey information by a decryption server in said downstream system, said decryption server being accessed only by authorization;

restoring said second encryption key by using either said set of passkeys or said passkey information so as to decrypt either said first encryption key or said first encryption key information and thereby restore said first encryption key;

using the restored encryption key to decrypt the received digital data;

locally generating a scramble key and a descramble key if the received digital data is successfully decrypted;

decoding the decrypted digital data to output restored digital data;

using the locally generated scramble key to scramble said restored digital data;

descrambling the scrambled digital data by an output device in said downstream system using the descramble key generated by said decryption server, said output device being accessed only by authorization; and

outputting from said output device the descrambled digital data in a predetermined output format.

6. A downstream system usable in an electronic data delivery system to output content, comprising:

a decryption server to which encrypted digital data is delivered, said decryption server including:

a decryption unit for decrypting said encrypted digital data;

a scramble control unit for locally generating a scramble key and a descramble key if the delivered digital data is successfully decrypted;

a content decoder for decoding the decrypted digital data to output restored digital data; and

a scrambler for scrambling said restored digital data with the locally generated scramble key; and

an output device coupled to said decryption server and including:

a descrambler for descrambling the scrambled, restored digital data with said descramble key generated in said decryption server; and

a signal processor for processing the descrambled digital data to a predetermined format and outputting the processed digital data as said content.

7. A decryption server usable in an electronic delivery system and to which encrypted digital data is delivered, comprising:

a decryption unit for decrypting said encrypted digital data;

a scramble control unit for locally generating a scramble key and a descramble key if the delivered digital data is successfully decrypted;

a content decoder for decoding the decrypted digital data to output restored digital data; and

a scrambler for scrambling said restored digital data with the locally generated scramble key.

8. An electronic circuit operable as a decryption server and usable in an electronic delivery system to which encrypted digital data is delivered, comprising:

a decryption unit for decrypting said encrypted digital data;

a scramble control unit for locally generating a scramble key and a descramble key if the delivered digital data is successfully decrypted;

a content decoder for decoding the decrypted digital data to output restored digital data; and

a scrambler for scrambling said restored digital data with the locally generated scramble key.

9. A storage medium for storing a computer-readable program that controls said computer to:

decrypt delivered, encrypted digital data;

generate a scramble key and a descramble key if the delivered digital data is successfully decrypted;

decode the decrypted digital data and output restored digital data; and

scramble the restored digital data with the generated scramble key.

10. A decryption server usable in an electronic delivery system and to which encrypted digital data is delivered, comprising:

a decryption unit for decrypting said encrypted digital data;

a content decoder for decoding the decrypted digital data to output restored digital data; and

a scrambler for scrambling said restored digital data with a predetermined scramble key to produce, as an output signal, scrambled decrypted digital data.

11. An electronic circuit operable as a decryption server and usable in an electronic delivery system to which encrypted digital data is delivered, comprising:

a decryption unit for decrypting said encrypted digital data;

a content decoder for decoding the decrypted digital data to output restored digital data; and

a scrambler for scrambling said restored digital data with a predetermined scramble key to produce, as an output signal, scrambled decrypted digital data.

12. A storage medium for storing a computer-readable program that controls said computer to:

decrypt delivered, encrypted digital data;

decode the decrypted digital data and output restored digital data; and

scramble the restored digital data with a predetermined scramble key to produce, as an output signal, scrambled decrypted digital data.

13. A decryption server usable in an electronic delivery system to decrypt digital data

that is delivered thereto and including a scramble control unit for generating a scramble key and a descramble key if the delivered digital data is successfully decrypted, said scramble key being used to locally scramble the decrypted digital data and the descramble key being used to locally descramble the scrambled digital data.

14. An electronic circuit operable as a decryption server and usable in an electronic delivery system to decrypt digital data that is delivered thereto and including a scramble control unit for generating a scramble key and a descramble key if the delivered digital data is successfully decrypted, said scramble key being used to locally scramble the decrypted digital data and the descramble key being used to locally descramble the scrambled digital data.

15. A storage medium for storing a computer-readable program that controls said computer to operate with a decryption server usable in an electronic delivery system to decrypt digital data that is delivered to the decryption server, the computer-readable program operating to control the computer to generate a scramble key and a descramble key if the delivered digital data is successfully decrypted, said scramble key being used to locally scramble the decrypted digital data and the descramble key being used to locally descramble the scrambled digital data.

16. An output device compatible with a decryption server in an electronic data delivery system and operable to output content, comprising:

a descrambler supplied with a descramble key by said decryption server for descrambling scrambled digital data provided by said decryption server; and

a signal processor for processing the descrambled digital data to a predetermined format and outputting the processed digital data as said content.

17. An electronic circuit that operates as an output device compatible with a decryption server in an electronic data delivery system and operable to output content, the

electronic circuit comprising:

a descrambler supplied with a descramble key by said decryption server for descrambling scrambled digital data provided by said decryption server; and

a signal processor for processing the descrambled digital data to a predetermined format and outputting the processed digital data as said content.

18. A storage medium for storing a computer-readable program that controls said computer to operate with a decryption server in an electronic data delivery system so as to output content, the program controlling the computer to descramble scrambled digital data provided by said decryption server by use of a descramble key supplied by said decryption server and to process the descrambled digital data to a predetermined format, thereby outputting the processed digital data as said content.

19. A method of recovering digital data supplied to a decryption server in an electronic data delivery system, the decryption server being accessed only by authorization and being operable to decrypt digital data that is encrypted in accordance with predetermined encryption keys, said method comprising the steps of:

locally generating in said decryption server a scramble key and a descramble key if the supplied digital data is successfully decrypted;

decoding the decrypted digital data;

using the locally generated scramble key to scramble the decoded digital data;

using, in an output device accessible only by authorization, the descramble key generated by said decryption server to descramble the scrambled digital data; and

outputting from said output device the descrambled digital data in a predetermined output format.

20. A method of scrambling digital data recovered by a decryption server to which encrypted digital data is delivered over an electronic delivery system, the decryption server

being accessed only by authorization, said method comprising the steps of:

locally generating in said decryption server a scramble key and a descramble key if the delivered digital data is successfully decrypted;

decoding the decrypted digital data; and

using the locally generated scramble key to scramble the decoded digital data.